

# INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2005/024374

**A. CLASSIFICATION OF SUBJECT MATTER**  
INV. H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/103281 A1 (BRICKELL ERNIE F) 27 May 2004 (2004-05-27) cited in the application the whole document	1-35
Y	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997, CRC PRESS LLC, USA, XP002394577 page 321 - page 322 page 330 - page 331 page 388 - page 390 page 394 - page 395 page 397 - page 398 page 472 page 515 - page 516 page 548 - page 552 ----- -/--	1-35

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

\* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search  11 August 2006	Date of mailing of the international search report  18/09/2006
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer  San Millán Maeso, J

# INTERNATIONAL SEARCH REPORT

International application No

PCT/US2005/024374

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>US 6 032 260 A (SASMAZEL ET AL)  29 February 2000 (2000-02-29)  abstract  column 2 - column 3</p>	1-35

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2005/024374

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004103281	A1	27-05-2004	
		AU 2003287567 A1	23-06-2004
		CN 1717895 A	04-01-2006
		EP 1566011 A1	24-08-2005
		JP 2006508608 T	09-03-2006
		WO 2004051923 A1	17-06-2004
US 6032260	A	29-02-2000	NONE

# PATENT COOPERATION TREATY

From the  
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

## PCT

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY  
(PCT Rule 43*bis*.1)

Date of mailing  
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference  
see form PCT/ISA/220

**FOR FURTHER ACTION**  
See paragraph 2 below

International application No.  
PCT/US2005/024374

International filing date (day/month/year)  
08.07.2005

Priority date (day/month/year)  
14.07.2004

International Patent Classification (IPC) or both national classification and IPC  
INV. H04L9/08

Applicant  
INTEL CORPORATION

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

### 2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:



European Patent Office - Gitschiner Str. 103  
D-10958 Berlin  
Tel. +49 30 25901 - 0  
Fax: +49 30 25901 - 840

Date of completion of  
this opinion

see form  
PCT/ISA/210

Authorized Officer

SAN MILLAN MAESO, J

Telephone No. +49 30 25901-477



**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.  
PCT/US2005/024374

---

**Box No. I Basis of the opinion**

---

1. With regard to the **language**, this opinion has been established on the basis of:
  - ☒ the international application in the language in which it was filed
  - ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).
2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:
  - a. type of material:
    - ☐ a sequence listing
    - ☐ table(s) related to the sequence listing
  - b. format of material:
    - ☐ on paper
    - ☐ in electronic form
  - c. time of filing/furnishing:
    - ☐ contained in the international application as filed.
    - ☐ filed together with the international application in electronic form.
    - ☐ furnished subsequently to this Authority for the purposes of search.
3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
4. Additional comments:

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US2005/024374

---

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

---

1. Statement

Novelty (N)	Yes: Claims	1-35
	No: Claims	
Inventive step (IS)	Yes: Claims	
	No: Claims	1-35
Industrial applicability (IA)	Yes: Claims	1-35
	No: Claims	

2. Citations and explanations

**see separate sheet**

**Re Item V**

**Reasoned statement with regard to novelty, inventive step or industrial applicability;  
citations and explanations supporting such statement**

1. Reference is made to the following documents:

- D1: MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography"  
1997, CRC PRESS LLC , USA , XP002394577**  
**D2: US 2004/103281 A1 (BRICKELL ERNIE F) 27 May 2004 (2004-05-27) cited in  
the application**

2. The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1-35 does not involve an inventive step in the sense of Article 33(3) PCT.

2.1. Independent claim 1

2.1.1. D1 consists of citations from the "Handbook of Applied Cryptography" which is a well-known textbook in the field of cryptography and discloses:

- (pages 548-551) establishing a protected on-line server to support key retrieval request from client computer systems;
- generating a key service public/private key pair for use in secure key retrieval processing;
- (pages 331 and 398) generating a pseudo-random value for a device;
- (pages 321, 322, 330 and 472) generating an encrypted data structure associated with a device, the encrypted data structure comprising a private key;
- (pages 397 and 398) generating an identifier, based on the pseudo-random value, for the encrypted data structure;
- (page 472) storing the identifier and the encrypted data structure on the protected online server; and
- (pages 397 and 398) storing the pseudo-random value and a hash value of the key service public key into non-volatile storage within the device.

2.1.2. Thus independent claim 1 cannot be considered as involving an inventive step because

it would be obvious (see PCT International Search and Examination Guidelines, Chapter 13, Paragraph 13.13) for the skilled man to combine the technical features of D1 together and other well-known technical features and/or design options in order to arrive at the subject-matter of claim 1.

**2.2. Independent claims 9, 17, 28 and 34**

The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 9, 17, 28 and 34, which therefore are also considered not inventive.

**2.3. Dependent claims 2-8, 10-16, 18-27, 29-33 and 35**

The features included in the above-mentioned dependent claims as far as they are not disclosed by D1 and/or D2 correspond to design options or are well-known in the field of Cryptography. It would therefore be obvious (see PCT International Search and Examination Guidelines, Chapter 13, Paragraph 13.13) for the skilled man to combine the teachings of D1 and D2 in order to arrive at the subject-matter of the dependent claims.

Therefore the subject-matter of claims 1-35 is not considered inventive in the sense of Article 33(3) PCT.

3. It is not at present apparent which part of the application could serve as a basis for a new, allowable claim.